

What is claimed is:

1. A computer security system, comprising:

(a) a non-volatile memory;

(b) a volatile memory; and

(c) a processor programmed to:

(1) detect exploitation of a computer operating system which is of a type that renders the computer insecure; and

(2) initiate a response to detection of said exploitation, which response entails at least one of:

(i) collecting forensics data characteristic of the exploitation; and

(ii) restoring the operating system to a pre-exploitation condition.

2. A computer security system according to claim 1 including a storage device.

3. A computer security system according to claim 2 wherein said storage device is removable..

4. A computer security system according to claim 1 wherein said response entails collecting forensics data characteristic of the exploitation, with the forensics data being transferred for storage onto a storage device.

5. A computer security system according to claim 4 wherein collection of said forensics data preliminarily includes halting all unnecessary processes on the computer and remounting all drives associated with said non-volatile memory.

6. A computer security system according to claim 1 wherein said forensics data is collected without utilizing resources of said non-volatile memory.

7. A computer security system according to claim 1 wherein said forensics data is collected in a manner which preserves integrity of non-volatile memory data.

8. A computer security system according to claim 1 whereby said forensics data is collected in a manner which preserves integrity of both volatile memory data and non-volatile memory data.

9. A computer security system according to claim 1 wherein said exploitation is selected from a group of comprises consisting of hidden kernel modules, hidden system call patches, hidden processes, and hidden files.

10. A computer security system according to claim 10 wherein said response entails restoring said operating system to a pre-exploitation condition by removing any hidden kernel modules, removing any hidden system call patches, terminating any hidden processes, and removing any hidden files which have been detected.

11. A computer security system, comprising:

(a) removable storage means;

(b) non-volatile memory;

(c) volatile memory; and

(d) processing means programmed for:

(1) detecting exploitation of a computer operating system which is of a type that renders the computer insecure; and

(2) initiating a response to detection of said exploitation, which response entails at least one of:

(i) collecting forensics data characteristic of the exploitation whereby it is stored on the removable media means; and

(ii) restoring the operating system to a pre-exploitation condition.

12. A computer security system according to claim 11 wherein collection of said forensics data preliminarily includes halting all unnecessary processes on the computer and remounting all drives associated with said non-volatile memory means.

13. A computer security system according to claim 11 wherein said forensics data is collected in a manner which preserves integrity of non-volatile memory data.

14. A computer security system according to any of claims 11 and 13 wherein said forensics data is collected in a manner which preserves integrity of volatile memory data.

5 15. A computer security system according to claim 11 wherein said exploitation is selected from a group of comprises consisting of hidden kernel modules, hidden system call patches, hidden processes, and hidden files, and wherein said response entails restoring said operating system to a pre-exploitation condition by removing any hidden kernel modules, removing an system call patches, terminating any hidden  
10 processes, and removing any hidden files which have been detected.

16. A computer-readable medium for use with a computer and having executable instructions for performing a method comprising:

(a) detecting exploitation of an operating system which renders a computer insecure; and

15 (b) initiating a response to detection of said exploitation, said response entailing at least one of:

(1) enabling transfer of data characteristic of the exploitation onto a removable storage device; and

(2) restoring the operating system to a pre-exploitation  
20 condition.

17. A computer-readable medium according to claim 16 wherein said removable storage device is an external flash drive.

18. A computer-readable medium according to claim 16 wherein the executable instructions accomplish halting of all unnecessary  
25 processes and remounting of all drives associated prior to data transfer.

19. A computer-readable medium according to claim 16 wherein the executable instructions enable data transfer in a manner which preserves integrity of non-volatile memory data on the computer.

30 20. A computer-readable medium according to claim 16 wherein the executable instructions enable data transfer in a manner which preserves integrity of volatile memory data on the computer.

21. A computer-readable medium according to claim 16 wherein the executable instructions enable data transfer in a manner which

preserves integrity of both volatile memory data and non-volatile memory data on the computer.

22. A computer-readable medium according to claim 16 wherein said exploitation is selected from a group of comprises consisting of hidden kernel modules, hidden system call patches, hidden processes, and hidden files.

23. A computer-readable medium according to claim 16 wherein the executable instructions enable restoration of said operating system to a pre-exploitation condition by removing any hidden kernel modules, removing any system call patches, terminating any hidden processes, and removing any hidden files which have been detected.

24. A computer-readable medium for use with a host computer that includes an associated operating system, non-volatile memory, and volatile memory, said computer-readable medium having executable instructions for performing a method comprising:

detecting an occurrence of exploitation to the operating system which renders the host computer insecure;

collecting, from said volatile memory, forensics data that is characteristic of the exploitation;

transferring said forensics data onto a removable storage device in a manner which preserves integrity of other data residing in said non-volatile memory; and

restoring the operating system to a pre-exploit condition.

25. A computer-readable medium according to claim 24 wherein said removable storage device is an external USB flash drive.

26. A computer-readable medium according to claim 24 wherein collection of said forensics data preliminarily includes halting all unnecessary processes on the computer and remounting all drives associated with said non-volatile memory.

27. A computer-readable medium according to claim 24 wherein the executable instructions enable collection of said forensics data in a manner which preserves integrity of volatile memory data.

28. A computer-readable medium according to claim 24 wherein the executable instructions enable collection of said forensics data in a

manner which preserves integrity of both volatile memory data and non-volatile memory data.

29. A computer-readable medium according to claim 24 wherein said exploitation is selected from a group of comprises consisting of hidden kernel modules, hidden system call patches, hidden processes, and hidden files and wherein the executable instructions enable restoration of the operating system to a pre-exploitation condition by removing any hidden kernel modules, removing an system call patches, terminating any hidden processes, removing any hidden files which have been detected.

30. A computer-readable medium according to claim 24 wherein said method is accomplished by a plurality of interfaced, loadable kernel modules which, collectively, contain the executable instructions.

31. A security software product for use on a host computer to monitor for, and respond to, activity corresponding to a rootkit exploitation which renders the host computer's operating system (OS) insecure, said security software product comprising:

(a) computer readable media having a suite of integrated software components adapted to interface with one another, said software components including:

(1) an exploitation detection component having executable instructions for detecting the activity corresponding to said rootkit exploitation;

(2) a forensics data collection component interfaced with said exploitation detection component for collecting forensics data characteristic of said rootkit exploitation so that said forensics data may be transferred to a removable storage device; and

(3) a OS restoration component interfaced with said exploitation detection component for restoring said operating system to a secure condition in response to detection of said activity.

32. A security software product according to claim 31 wherein said exploitation detection component is capable of detecting signature-

based on non-signature-based activity corresponding to a rootkit exploitation.

33. A security software product according to claim 31 wherein said activity is selected from a group of compromises consisting of hidden kernel modules, hidden system call patches, hidden processes, and hidden files, and hidden ports.

34. A security software product according to claim 31 system wherein said forensics data collection component is operative to preliminarily halt unnecessary processes on the computer and remount all drives associated with the computer's non-volatile memory.

35. A security software product according to claim 31 wherein said forensics data collection component is operative to collect forensics data without using non-volatile memory resources, while preserving integrity of volatile memory data.

36. A security software product according to claim 31 wherein said OS restoration component is operative to remove any hidden kernel modules, remove any system call patches, remove any hidden files, and to terminate any hidden processes detected by said exploitation detection component.

37. A security software product for use on a host computer running a Linux operating system to monitor for, and respond to, activity corresponding to a rootkit exploitation which renders the host computer insecure, said security software product comprising:

(a) a computer readable medium having a plurality of integrated software components adapted to interface with one another, said software components including:

(1) a first loadable kernel module having associated first executable instructions for detecting an occurrence of said rootkit exploitation;

(2) a second loadable kernel module interfaced with said first kernel module, and having associated second executable instructions for collecting forensics data characteristic of said rootkit exploitation and for enabling

said forensics data to be transferred for storage onto a removable storage device; and

(3) a third loadable kernel module interfaced with said first kernel module, and having associated third executable instructions for restoring said operating system to a secure condition in response to detection of said rootkit exploitation by said first kernel module.

38. A security software product according to claim 37 system wherein said second loadable kernel module is operative to preliminarily halt unnecessary processes on the computer and remount all drives associated with the computer's non-volatile memory.

39. A security software product according to claim 31 wherein said forensics data collection component is operative to collect forensics data without using non-volatile memory resources, while preserving integrity of volatile memory data, and wherein said OS restoration component is operative to remove any hidden kernel modules, remove any system call patches, remove any hidden files, and to terminate any hidden processes detected by said exploitation detection component.

40. A computerized method, comprising:

(a) monitoring activity within a computer operating system in order to detect occurrence of an exploitation which renders the computer insecure, and thereafter performing at least one of:

(1) collecting forensics data characteristic of the exploitation in a manner which preserves integrity of characteristic information stored in both non-volatile and volatile memory resources of the computer; and

(2) restoring the operating system to a pre-exploitation condition.

41. A computerized method according to claim 40 comprising transferring said forensics data located in volatile memory resources on the computer onto a removable storage device.

42. A computerized method according to claim 40 whereby forensics data located with said volatile memory resources is collected prior to powering down the computer.

43. A computerized method according to claim 40 comprising preliminarily halting all processes on the computer and remounting all drives associated with said non-volatile memory.

5

44. A computerized method according to claim 40 comprising monitoring activity relating attempts to hide kernel modules, system call patches, processes, and files.

10

45. A computer security system according to claim 40 whereby restoration of the operating system is accomplished removing any hidden kernel modules, removing an system call patches, terminating any hidden processes, and removing any hidden files.